ABSTRACT

A digital ticket is procured by a client ticket consumer upon, preferably, the Internet from and by staged interaction with a ticket provider server. The digital ticket becomes embodied in a tangible transportable data storage medium, normally a 2-D bar code printed on paper by the consumer, or on the consumer's flexible disk or smart card, containing **Sign(s,I||hash(R))||R** where (1) **R** is a number having its origin in the computer of the ticket consumer, which number R is appended to (2) a number **Sign(s,I||hash(R))**. This number **Sign(s,I||hash(R))** was earlier computed in the computer of the ticket provider as a digital signature using signature key **s** of a number **hash(R)** combined with event information **I**, and was subsequently communicated across the communications network to the computer of the ticket consumer. The number **hash(R)** was itself even earlier computed in the computer of the ticket consumer as a one-way function of random number **R**, which computed one-way function was subsequently communicated to the computer of the ticket provider. The number **R** is private to the ticket consumer and not public; the digital signature key **s** is private to the ticket provider.

The digital ticket is redeemed by (1) transporting the transportable storage medium within which the **Sign(s,I||hash(R))||R** is written to the particular selected event; (2) tendering the digital ticket for verification and for admission; (3) reading the **Sign(s,I||hash(R))||R** to an event computer and extracting the number **R**; (4) decrypting the remaining **Sign(s,I||hash(R))** with verification key *v* of the ticket producer to get **hash(R)** and **I**; (5) re-calculating from **R**, with the same one-way function previously used, a re-calculated **hash(R)**; then, having this recalculated **hash(R)** to hand; (6) comparing the re-calculated **hash(R)** to the extracted **hash(R)**. The (4) decrypting will work, producing a proper **I** for the selected event~~, and the~~ (6) comparing will be equal, only for a legitimate ticket.